Pentesting application on iPhone

With jailbreak

It is possible to get a application working without rooting it. BUUUT you need a developer certificate. You can get a temprorary though, for just a few days. SO you can certify the application, then send it to the phone.

With Checkra

After rooting the device, open up the Checkra icon. And install Cydia.

Openssh

Open Cydia and search for OpenSSH. Install it. It is a console app so there is no icon for it. Once it is installed you can access it over SSH. So just run root@iphone-ip-address. The default password is `alpine`.

Ipainstaller

With cydia you can install `ipainstaller`.

Extracting ipa files

With `ipainstaller` you can extract it like this: First list all packages: `ipainstaller -l`. Then identify the package, and do `ipainstaller -b the.app.com`.

Then use scp to transfer it to your machine.

```
scp root@10.0.0.1:/private/var/mobile/Documents/package.ipa ./
```

Without jailbreak

Getting the application onto the phone

If the device is rooted you can simply go to Re-activate JB. Click "GO", and then follow the instructions.

Once that is done you want to enable ssh, in order to install the ipa. So you go to "Toggle SSH" and enable ssh deamon. Now you can log in to the mobile over ssh with the root-account, and the password that is on the backside of the phone.

To install an ipa you can use the command "ipainstaller". It can be downloaded thgouh cydia.

- Trust the developer

AFter the application has finished installing it should pop up among your applications on the phone. When you try to open it it might be denied because Apple does not trust the developer of the application. To solve that problem you go to Settings/General/Profiles and Device Management/ and then click on the developer of the application. ANd then add "Trust".

- BankdID

If you proxy all traffic through burp, burp will intercept traffic to the bankid servers. Since the bankid application has certificate pinning, you cannot intercept that traffic. Instead the traffic won't be sent at all. So in order to fix that if your application requrires BankID you can add SSL Passthrough in burp. So that Burp won't intercept traffic to specific host.

You do that by going to Proxy/Options/SSL Passthrough Then add: `.*bankid.com.*$`